Open Dialogue Foundation
Brussels | Warsaw | Kyiv | Miami
HQ: Rond-point Schuman 6/5
1040 Brussels, Belgium

Bruxelles, 11 giugno 2025

SLAPP e repressione finanziaria transnazionale in Belgio/UE e negli Stati Uniti:

il caso contro Lyudmyla Kozlovska e la Fondazione Open Dialogue

Nel 2022, i servizi speciali del Kazakistan hanno orchestrato una denuncia penale collettiva in Belgio contro la Fondazione Open Dialogue e la sua presidente, l'attivista per i diritti umani Lyudmyla Kozlovska. Gli agenti, presentando denunce per conto dei loro figli minorenni, hanno accusato la Fondazione e la sua presidente di molestie, diffamazione e cyberbullismo. Si sono atteggiati a vittime e hanno chiesto la rimozione dai social media dei video pubblicati dalla Fondazione che documentavano il loro coinvolgimento nella repressione politica, nella tortura e in uccisioni in Kazakistan.

Il tribunale del Belgio ha infine archiviato il procedimento contro la Fondazione e la sua Presidente, dichiarando che il Belgio non aveva giurisdizione territoriale sui presunti reati. I documenti del tribunale belga rivelano che le autorità kazake, avvalendosi di questi agenti che si fingevano cittadini comuni pur essendo membri attivi della polizia e dei servizi di vigilanza del Kazakistan, hanno cercato di ottenere dati di sorveglianza personale dettagliati sia sulla Fondazione che sulla Kozlovska in tutto il Belgio/UE e negli Stati Uniti, tra cui:

1. Dati completi del passaporto e cronologia dei viaggi della Kozlovska, in particolare i suoi spostamenti tra il Belgio e gli Stati Uniti.
2. Dettagli dei suoi voli e attraversamenti delle frontiere negli aeroporti belgi all'interno della zona Schengen.
3. Informazioni finanziarie complete, tra cui:
    - Transazioni bancarie complete,
    - Fonti di finanziamento per i suoi viaggi e alloggi.
4. Corrispondenza e-mail privata tra Kozlovska e la Fondazione durante i suoi soggiorni in Belgio e negli Stati Uniti.
5. Dettagli operativi interni della Fondazione, compreso il modo in cui Kozlovska gestiva le attività durante i viaggi.
6. Dati tecnici dei video registrati da Kozlovska, tra cui:
    - File multimediali grezzi, registrazioni e fotografie,
    - Date di creazione e pubblicazione,
    - Dettagli sulla proprietà delle attrezzature e sui finanziamenti,
    - Nomi del personale amministrativo.

Il giudice istruttore belga ha affermato esplicitamente che tali richieste sembravano volte a "utilizzare la giustizia belga per raccogliere il massimo di dati personali e privati su Kozlovska possibile per scopi diversi dalla semplice rivelazione della verità in questo caso".

Questo caso illustra due tattiche che minano lo Stato di diritto e l'integrità finanziaria e della sicurezza informatica dei paesi democratici:

1. Strategic Lawsuit Against Public Participation (SLAPP) – Una tattica ben conosciuta di contenzioso abusivo rivolta contro giornalisti e difensori dei diritti, basata sull'articolo 81,

paragrafo 2, lettera f), del trattato sul funzionamento dell'Unione europea e adottata con la cosiddetta direttiva anti-SLAPP (direttiva (UE) 2024/1069)[1].

2. Transnational Financial Repression – Una nuova tattica, che consiste nell'uso improprio e nella manipolazione deliberata dei quadri normativi finanziari internazionali da parte di governi stranieri o attori non statali, allo scopo di mettere a tacere, intimidire, sorvegliare o reprimere in altro modo individui, organizzazioni o entità al di fuori della loro giurisdizione territoriale. Questi quadri normativi, sviluppati sulla base delle raccomandazioni del Gruppo di azione finanziaria internazionale (GAFI), includono le leggi antiriciclaggio (AML), le normative contro il finanziamento del terrorismo (CFT), e le leggi sulla sicurezza informatica e i trattati di assistenza giudiziaria reciproca (MLAT). Le forme di repressione finanziaria transnazionale includono, ma non si limitano a, azioni volte al congelamento o alla confisca ingiustificati di beni, alla privazione dell'accesso ai servizi finanziari, allo sfruttamento delle informazioni finanziarie e dei dati personali, alla diffusione di disinformazione mirata per minare la reputazione economica di un'entità e all'avvio di procedimenti legali motivati da ragioni politiche (SLAPP). Questa forma di repressione transnazionale viola il principio fondamentale della fiducia reciproca insito nella cooperazione internazionale in materia di normative AML/CFT e altri trattati di sicurezza. Compromette i diritti umani fondamentali, la sicurezza nazionale ed economica, l'integrità finanziaria e lo Stato di diritto dell'UE e dei suoi alleati.

Claude Moniquet, ex ufficiale dei servizi segreti francesi e attuale capo dell'European Strategic Intelligence and Security Center (ESISC)[2] — una società privata di intelligence e lobbying con sede in Belgio — ha svolto un ruolo fondamentale in questo procedimento. Il 1° luglio 2022, Moniquet ha presentato la denuncia penale contro Kozlovska e la Fondazione Open Dialogue, agendo in qualità di rappresentante legale degli agenti di polizia kazaki e dei loro figli attraverso una procura rilasciata da un avvocato kazako.

I documenti del caso dimostrano che il contributo di Moniquet ha facilitato le richieste di raccolta di dati su vasta scala. Le azioni legali coordinate da Moniquet erano strategicamente progettate per proteggere gli agenti e le forze dell'ordine kazaki dal controllo internazionale in materia di violazioni dei diritti umani, raccogliendo al contempo informazioni sui difensori dei diritti umani che operano nelle democrazie occidentali.

Nella decisione del tribunale del 13 dicembre 2023, il giudice istruttore belga ha specificatamente osservato che alcune azioni investigative richieste dalle "vittime" sembravano intese a "strumentalizzare la giustizia belga" per scopi che andavano oltre l'accertamento dei fatti rilevanti.

Vale la pena notare che l'organizzazione di Moniquet, ESISC, era già stata indagata per presunta corruzione all'interno dell'Assemblea parlamentare del Consiglio d'Europa (PACE) nel periodo 2017-2018 in relazione ad attività illegali di lobbying a favore dell'Azerbaigian (nel caso della "diplomazia del caviale").[3]

[1] https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-initiative-against-abusive-litigation-targeting-journalists-and-rights-defenders
[2] https://www.esisc.org/about-us/our-mission
[3] https://assembly.coe.int/Communication/IBAC/IBAC-GIAC-Report-EN.pdf

Il caso evidenzia un preoccupante modello di abuso del quadro normativo in materia di sicurezza informatica e AML/CFT, sviluppato sulla base delle raccomandazioni del GAFI, e l'urgente necessità di una riforma:[4]

1. **Utilizzo improprio dei requisiti di trasparenza finanziaria**: le parti legate al Kazakistan hanno tentato di utilizzare accuse vagamente formulate in merito ad attività finanziarie sospette per commettere molestie, diffamazioni e cyberbullismo come pretesto per richiedere una vasta documentazione finanziaria. Ciò rappresenta un tentativo diretto di abusare dei principi alla base delle Raccomandazioni 10 (Due diligence sul cliente Due Diligence) e 20 (Segnalazione di operazioni sospette) del GAFI per una sorveglianza motivata da ragioni politiche piuttosto che da legittime preoccupazioni relative alla criminalità finanziaria.
2. **Abuso dei meccanismi di condivisione transfrontaliera delle informazioni:** la richiesta di dettagliati estratti conto bancari e attività transazionali sfrutta i meccanismi di cooperazione internazionale istituiti ai sensi delle Raccomandazioni 37 e 40 del GAFI, che sono stati concepiti per legittimi scopi di applicazione della legge piuttosto che per colpire i dissidenti.
3. **Appropriazione impropria del quadro normativo contro il finanziamento del terrorismo:** i documenti del tribunale dimostrano che i meccanismi standard di controllo finanziario volti a prevenire il finanziamento del terrorismo sono stati riutilizzati per monitorare i difensori dei diritti umani, compromettendo direttamente lo scopo previsto dalla Raccomandazione 6 del GAFI.
4. **Sfruttamento delle lacune giurisdizionali:** il tentativo di utilizzare i canali legali belgi per accedere ai dati finanziari statunitensi dimostra come i regimi autoritari sfruttino le differenze nell'attuazione nazionale degli standard GAFI per cercare la giurisdizione più vantaggiosa.
5. **Inversione del quadro normativo relativo alle persone politicamente esposte (PPE):** anziché utilizzare una due diligence rafforzata per monitorare i funzionari corrotti (come previsto), il caso illustra come il quadro normativo relativo alle PPE possa essere invertito per consentire a tali funzionari di prendere di mira i propri critici in giurisdizioni quali il Belgio e gli Stati Uniti.

Questo caso fornisce prove concrete di come i quadri normativi internazionali in materia di finanza e sicurezza informatica vengano sfruttati. Anziché combattere la criminalità finanziaria o informatica come previsto, questi sistemi vengono utilizzati in modo improprio per consentire la repressione finanziaria transnazionale e le tattiche SLAPP. Questo abuso mina lo Stato di diritto, la sicurezza nazionale e l'integrità finanziaria dei paesi occidentali che questi quadri normativi erano stati concepiti per proteggere. Dimostra inoltre che, una volta che le richieste di dati entrano nel sistema giudiziario, la vita privata dei cittadini e dei residenti del Belgio/UE e degli Stati Uniti è già a rischio.

Per ulteriori informazioni, contattare:

Lyudmyla Kozlovska, Presidente della Fondazione Open Dialogue
E-mail: lyudmylakozlovska@odfoundation.eu

[4] https://www.fatf-gafi.org/content/dam/fatfgafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf